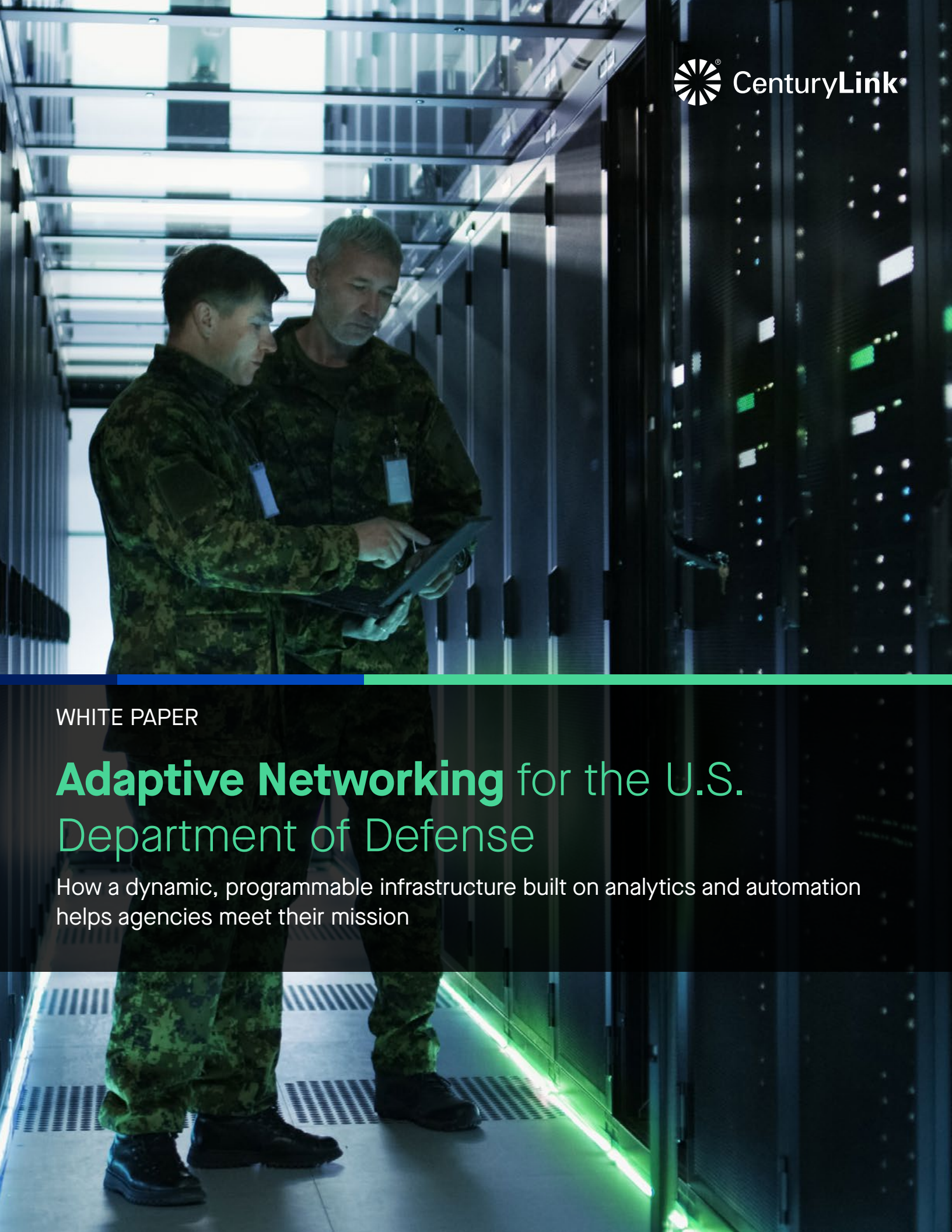


CenturyLink

WHITE PAPER

# **Adaptive Networking** for the U.S. Department of Defense

How a dynamic, programmable infrastructure built on analytics and automation helps agencies meet their mission

U.S. military forces and their partners need to be able to adapt their networks to a constantly morphing, asymmetric and unpredictable threat landscape. Their network needs to be able to collect and analyze reams of data from all sorts of sources—whether from troops on the ground, drones in the air or network data. And it needs to be able to be deployed quickly when necessary and tailored to the parameters of any given operation—all the while ensuring that its systems are secure and the information it provides is reliable. One approach that can help make the U.S. Department of Defense's IT plans a reality is the adaptive network.

# Enabling your agency's mission with Adaptive Networking

An army may march on its stomach, as the old adage goes, but it runs on its network. Especially these days, when military actions invariably involve joint forces and coalition partners, crucial activity in multiple domains, and adversaries that are utilizing advanced technologies. America's military forces need a comprehensive network that is secure and able to synthesize and analyze data from a wide array of sources and to be able to quickly give commanders a complete view of what's happening in real time. It must not only be fast, but also able to be deployed quickly anywhere in the world.

The Department of Defense (DOD) is working hard to meet those demands in its ongoing efforts toward IT modernization, though leadership acknowledges that they still have some work to do.

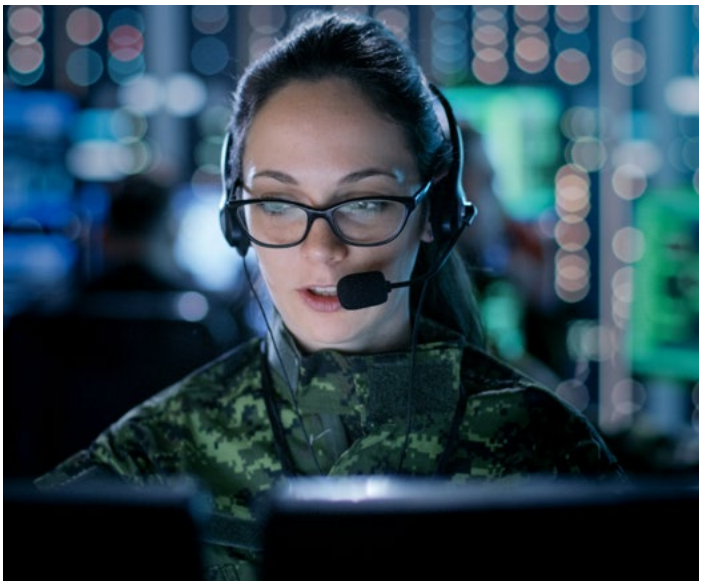
"Today, we are emerging from a period of strategic atrophy, aware that our competitive military advantage has been eroding," the 2018 National Defense Strategy states in laying out the global threat landscape. As the focus has shifted from the wars in Iraq and Afghanistan to more complex scenarios involving China, Russia, North Korea, Iran and others, the challenge is marked by technological modernization.

**"Today, we are emerging from a period of strategic atrophy, aware that our competitive military advantage has been eroding."**

- Excerpt from 2018 National Defense Strategy

"This increasingly complex security environment is defined by rapid technological change, [and] challenges from adversaries in every operating domain," the report reads.

The document, which maps out the DOD's plans through 2023, outlines a number of priorities. Among them is developing "a lethal, agile and resilient force" that can respond quickly and effectively in an uncertain world. According to the report, "much of our force employment models and posture date to the immediate post-Cold War era, when our military advantage was unchallenged and the primary threats were rogue regimes." Those models will give way to a Dynamic Force Employment concept that will "more flexibly use ready forces to shape proactively the strategic environment while maintaining readiness to respond to contingencies and ensure long-term warfighting readiness."



# The case for Adaptive Networking

In many ways, the DOD's goals describe the approach taken by Adaptive Networking.

For the DOD, an adaptive network provides the flexibility to support activities for forces, as they are deployed, expanding or contracting in functionality to accommodate whatever task may be at hand. Its software-driven approach can accommodate multiple cloud environments while providing automated management and analysis, and end-to-end security from a centralized location.

**"The essence of technology isn't the technology itself, but 'How do I use 5G to support the mission.'"**

- Dr. Leslie Perkins, U.S. Air Force chief of cybersecurity

CenturyLink Adaptive Networking solutions bring the physical and virtual layers of a network together in real time. It gathers information from any number of sources, including users, sensors, applications and other sources, and sends it to a software layer then analyzes that data and recommends action without slowing down the network itself. Meanwhile, it provides fine-grained network monitoring to maintain optimum performance and draws on a large global network to support security efforts by identifying and mitigating cyberthreats.

Computer-based networks have evolved over the years, transitioning from a static infrastructure to autonomous networks capable of configuring, monitoring and maintaining themselves without much human intervention. But even autonomous networks have their limits in terms of flexibility and adapting to a changing environment. Adaptive Networking takes the next step in the evolution, bringing intelligent automation to bear on aspects such as intent-based orchestration, analytics and programmable domain control. It can scale to meet the demands of a growing operation and has the elasticity to conform to specific configurations. It also enables a DevOps approach to software development and operations, shortening the development lifecycle to provide operational and service agility.

## This approach is built on three key layers

### Programmable infrastructure

Covering a network's physical and virtual elements, the programmable infrastructure includes a flexible grid, a reconfigurable optical layer that allows for rerouting, and the ability to correlate telemetry from the IP layer with routing data. The result is an intelligent layer capable of interpreting data and making adjustments, from routing traffic around a downed circuit to investigating the cause of unexpected low latency or capacity.

### Analytics and intelligence

The ability of analytics software to handle big data is well known and getting better all the time, thanks to technologies like artificial intelligence and machine learning. CenturyLink Adapative Networking has the capacity to manage and analyze massive amounts of data, looking for patterns or vulnerabilities and recommending action. But it also pays attention to the small data that shows up as the equivalent of faint beeps or small gestures amid the roaring noise of operations that nevertheless signal the need for immediate action. Whether it's a small technical problem with a circuit or a request from a user, the analytics layer can respond quickly.

### Software control and automation

Software-defined networking and multi-domain service orchestration allow an adaptive network to deliver network management and services across multi-vendor, multi-domain hybrid networks. Automation, while performing tasks such as traffic optimization and network monitoring, also prevents a lot of human error, which is still the clear leader among causes of network outages, according to Dimensional Data's most recent global study. Of the respondents in that study, 97 percent admitted that human factors were responsible for at least some of their outages, with nearly half saying humans played a part frequently. In addition to everything else it provides, automation helps prevent a lot of downtime.

Physically, an adaptive network is like an appliance, but its programmable software allows it to adapt to circumstances. It can be up and running quickly, through its APIs and modern data models that allow organizations to customize their infrastructure to fit specific needs. The APIs can be used at both the hardware and software layers to improve real-time network telemetry and measurement. The APIs also integrate easily with IT tools, thus allowing for multi-platform and multi-vendor application development that makes more efficient use of IT resources.

Approx. **450,000** global route miles of fiber

**150,000+** on-net buildings

**Global Network Footprint**

# The big picture

Networks are only as good as their weakest links, and Adaptive Networking can keep close tabs on a network's health, both in terms of operational functionality and cybersecurity. It starts with a holistic view of network and how it serves the mission.

For the DOD, the guiding principle behind technology modernization is to look at technology not as an end in itself, but as the means of achieving the department's goal of supporting the warfighter, noted Dr. Leslie Perkins, the chief of cybersecurity support for the U.S. Air Force. The essence of 5G wireless, for example, isn't the technology itself, but, "how do I use 5G to support the mission," said Perkins, who recently spoke on an industry panel that included CenturyLink.

The integrity of any new technology is also critical. As networks expand to cover greater geographic expanses and a proliferating variety of components, it's important to keep track of the underlying elements, such as network transport, data security and the system's data flows. This is done to ensure that the system is not just operational, but that the data and analysis it's providing are trustworthy. That comes from having a broad, holistic view of a network and its components, with security built in at the beginning rather than tacked on. A holistic view is necessary because of the interconnected nature of modern networks, which include communications between command posts and deployed units, operation of unmanned air, sea and ground vehicles, and the data pouring in from all those assets, as well as from mobile devices, IoT sensors and other data sources around the world.

In terms of cybersecurity, Adaptive Networking can draw on the expansive CenturyLink global fiber network. Being able to see more information on current threats from around the globe significantly increases the chances of identifying an incoming attack and mitigating it.

## Visibility and expertise to see more and to stop more

Because of our expansive inside out view of the global internet, CenturyLink has an extensive raw data platform as the foundation to derive actionable threat intelligence. This comprehensive access to dynamic global data powers our ability to predict, identify and monitor threats around the world.

### See more

We have the data platform for visibility into 114 billion NetFlow sessions ingested and analyzed per day.

**~771 million DNS queries collected per day.**

### Analyze more

Every day our security experts tackle the complexity of protecting one of the world's largest IP backbones 24/7. The validation and original threat discovery done by our threat research team, Black Lotus Labs, drive the fidelity of our intelligence.

**During 1H19, Black Lotus Labs tracked 18,000+ C2s daily.**

### Stop more

Because of our highly distributed network edge, we efficiently shift the first line of defense closer to the threat source. Our global network acts as a proactive defense platform, blocking malicious activity before it impacts the customer environment.

**We block upstream attacks, mitigating more than 14,000 DDoS attacks in 1H19.**

# Locking down data

To say the DOD has a complex network is a massive understatement. It's a worldwide network operating across all domains—land, sea, air, space and cyberspace—with a mix of cloud systems, operating procedures and architectures, a vast array of hardware and software, and countless sensors, communications systems and multi-function mobile devices operating on both classified and non-classified systems.

Securing such an environment in many cases involves a patchwork of firewalls, antivirus and intrusion detection systems. Other security procedures and policies can provide protection in certain areas, but also leave gaps and vulnerabilities, especially when critical communications and information are extended all the way to the edge during deployment situations.

An adaptive network instead uses a multi-layered, network-based approach that provides the visibility and flexibility necessary to confront the ever-changing threat landscape. The same approach that is used to manage the network can be applied to securing it and its data. Its consolidated portal provides a clear view of a network's components and activity and can draw on security reports and data from one of the world's largest IP backbones to provide a comprehensive view of active threats and identify attacks to the network.

In this way, the network acts as a sensor; monitoring, detecting, blocking and reporting attempts to infiltrate the network. An adaptive network includes a full slate of security features—including intrusion detection and prevention, web content and URL filtering, application awareness and control, anti-malware (sandboxing) and data loss protection. A high-level of encryption protects communication from end to end without slowing down network performance. And through a distributed design that moves protection closer to the endpoints, it can mitigate threats much more quickly than traditional networking. It's also carrier-independent, able to work with third-party providers and hybrid networks.

Automation provides speed and a comprehensive, analytics-driven view of the network, which when combined with its other features, allows organizations to be proactive in their defense. That centralized control, adaptability and presence near the network edge also can help implement a new focus on identity management as one key to better security. The DOD, like other sectors, is moving away from focusing on the network perimeter to focusing on authenticating users and devices on an ongoing basis in order to improve security. The department's Identity and Access Management (IdAM) program is a DOD-wide program focusing on a continuous process of managing digital identities, authenticating users and authorizing access to resources. Like other organizations, the DOD eventually wants to get to a zero trust networking model.

**CenturyLink named a Visionary in Gartner 2019 Magic Quadrant for Managed Security Services, Worldwide**

| | | |
|---|---|---|
| Black Lotus Labs' systems, on average, monitored for **~1.2M** unique threats daily during the first half of 2019 | These threats represent **~15M** distinct malicious indicators tracked during the same timeframe | Black Lotus Labs takes down **~63 C2s** per month from the CenturyLink Network |

# The meaning of modernization

Modernization is more than new technology and equipment. It involves a hefty dose of cloud computing and an emerging use of artificial intelligence, sure. It also incorporates improvements to satellite communications and an eventual move to 5G wireless technologies, along with fleets of autonomous vehicles, IoT devices and a host of other improvements. But the ultimate goal for the DOD is to serve the warfighter and support the mission in any location and environment. It is, according to David Bennett, CIO and director of operations for the Defense Information Systems Agency (DISA), "about cyber survivability."

Bennett, making the keynote address at a recent industry briefing in Arlington, Va., discussed some of his plans for the DOD networks, including solving a lack of interoperability among some of the department's components and far-flung commands, and eliminating single points of failure in its networks. But he also stressed that the bottom line of IT modernization is to deliver reliable, trustworthy and effective tools to units in the field.

"The only view that counts is the end-to-end view," Bennett said. That view is complicated by a lack of interoperability, for instance, among different commands in the United States,

Asia, Europe and elsewhere that affects joint operations and, particularly, coalition partners. DISA is trying to merge systems to increase interoperability and eliminate single points of failure. An example is the consolidation of the 14 Fourth Estate agencies—those that serve the DOD, but they aren't tied to a particular military service—under cloud. Those 14 agencies have 14 IT environments, in both in-house and commodity products. With the consolidation, DISA will give them one way of thinking, Bennett said.

A cloud-based adaptive network that functions independently of the underlying platform can, in certain circumstances, alleviate some of the problems of interoperability.

The key is developing a culture of being proactive in meeting IT challenges, rather than focusing too much on the technology alone, he said. Modernization isn't just a matter of new hardware, software or the latest whiz-bang apps, he said. The primary focus should always be on supporting the mission, which depends on how services and solutions are implemented and managed. "Technology is not the answer," Bennett said. "It is the culture."

**"Modernization is more than new technology and equipment. It is "about cyber-survivability."**
- David Bennett, CIO and director of DISA operations

Part of the culture is how policy deals with the risk questions: How am I allowed to react to an attack, particularly when lives are at stake? Are shutdowns worth it, and when, in what situations? What are the criteria? An automated, intelligent network with centralized control can deliver the kind of visibility necessary for answering those questions.

## Flexible management

Not least among the advantages of Adaptive Networking is the ability to make changes to a network on the fly, which has become a priority as much in a business setting as in a military setting. In a recent enterprise WAN survey by Frost & Sullivan, 61 percent of IT decision-makers rated the ability to make changes quickly as a top criterion. Among other priorities in the survey: improving productivity (81 percent), network and application security (77 percent), and the ability to apply granular security policies (76 percent). Adaptive Networking gives organizations the agility to deploy bandwidth as needed, improve their security posture and apply policies via centralized control.

## Moving forward

A point consistently driven home by defense leadership is that IT modernization is not an end state. It's a process of continual change and improvement. By modernizing with an adaptive network, which by design is geared toward changes and improvements, the DOD could help ensure that it continues meeting the modernization needs of today's warfighter.